

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION**

UNITED STATES OF AMERICA	§	
	§	
V.	§	Criminal No. 4:20-cr-00455
	§	
ZHENG DONG CHENG	§	

**UNITED STATES’ RESPONSE TO DEFENDANT’S REPLY TO UNITED
STATES’ RESPONSE TO DEFENDANT’S MOTION
TO SUPPRESS**

The United States of America, by and through Jennifer Lowery, Acting United States Attorney for the Southern District of Texas, and Carolyn Ferko and S. Mark McIntyre, Assistant United States Attorneys, and Matthew McKenzie, Trial Attorney, files this response to the Defendant’s Reply to the United States’ Response to Defendant’s Motion to Suppress, and would show the following:

I. Defendant’s Reply To the United States’ Response

The Defendant submitted a reply to the United States’ response which repeats arguments made in the initial Motion to Suppress. The Defendant claims the United States “focuse[d] on arguments Cheng did not make and ignores those Cheng did make.” (Defendant’s Reply at p. 1). The United States requests that this Court review the arguments presented as the United States has answered the points made

by the Defendant. The United States submits that the Defendant Cheng waived his rights and knowingly consented to the search of his electronic devices by voluntarily providing the Special Agents with the passwords for the devices. However, should the Court disagree with that position, the United States concedes that clarification may be required for the issue of the electronic device passwords which will be discussed herein.

II. Irrespective of Consent, the Evidence Found on the Defendant's Electronic Devices Was Lawfully Obtained Pursuant to Valid, Executed Search Warrants, Issued by a U.S. Magistrate Judge

The Defendant asserts the Special Agents' conduct during the custodial interrogation renders the Defendant's consent invalid. (Defendant's Reply at pp. 3-5). The Defendant alleges that as a result of the invalid consent, the passwords provided were "fruit of the poisonous tree." That assertion is just not the case.

The Defendant declares that "[w]ithout the passwords, which are part of Cheng's statements to be suppress, no copying/imaging and searches (contemporaneous or subsequent) would have been possible due to device encryption or other security features." (Defendant's Reply at p. 4). This statement is patently incorrect as courts have held that should valid search warrants be issued, defendants can be compelled to provide access to electronic devices.

“[A] warrant is generally required before [searching the contents of an electronic device], even when [an electronic device] is seized incident to arrest.” *Riley v. California*, 573 U.S. 373, 401 (2014) (“Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple – get a warrant.”); *See also Carpenter v. United States*, 138 S. Ct. 2206 (2018). Once a warrant has been issued, courts may issue decryption orders so as to access requisite evidence pursuant to Rule 41 of the Federal Rules of Criminal Procedure and the All Writs Act. *See* 28 U.S.C. § 1651(a) (“The Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law.”); *See also United States v. Apple Mac Pro Comp.*, 949 F.3d 102, 116 n. 5 (3d Cir. 2020).

“The exclusionary rule, which permits criminal defendants to seek exclusion (suppression) of evidence obtained through illegal search and seizure” has been characterized by the Supreme Court as “an extreme sanction that courts should apply only sparingly.” *United States v. Ricks*, No. 4:18-CR-00197-MAC-CAN, 2019 U.S. Dist. LEXIS 59859, *11 (E.D. Tex. 2019) (citing *United States v. Leon*, 468 U.S. 897, 926 (1984)). Therefore, when a warrant has been obtained, as here, exclusion of evidence would be a sanction disproportionate to any violations alleged by the Defendant.

The Defendant was arrested and detained on August 23, 2020 in the early evening hours, Central Time. Specifically, once the Special Agents were provided the passwords by the Defendant, the agents passed them on to the members of the FBI Regional Computer Forensics Laboratory (“RCFL”) team who, for the two cellular phones and one iPad, verified the passcodes that were provided by the Defendant were accurate. Once the passcodes were verified, the RCFL team put the devices into “airplane” mode. See Exhibit A, p.1. For the Lenovo laptop, the team was asked to verify if there was any encryption, and if so, was it currently up and running since the laptop was seized in the “powered-on” state. See Exhibit A, p.2. There was no encryption. That was all that was done to the above referenced devices until the search warrants were approved on the 27th and 28th.

As previously stated in the United States’ response, separate search warrants were authorized for each electronic device confiscated from the Defendant at the time of his arrest. On August 27th and 28th, approximately four days after the lawful arrest of the Defendant and seizure of the electronic devices, search warrants were issued for each of the individual items and devices: a Black Swiss Gear Backpack, a Black Samsonite Soft Sided Roller Bag and a Teal Samsonite Hard Sided Roller Bag, one Huawei Smart Phone (IMEI1: 865594046461105), one Samsung Smart Phone (IMEI: 359301100386605), one Apple iPad (S/N: F9FTG5BPHLFC), one Lenovo ThinkPad (S/N: PK0M1E313/08), one Western Digital Hard Drive

(S/N:Unreadable), and one Western Digital Hard Drive (S/N: WXQ1A87HLVC6)). The warrants were authorized by United States Magistrate Andrew M. Edison on August 27th and 28th, 2020¹. The Search Warrants did not request passwords/biometrics since they were already provided by the Defendant and the devices were in “airplane” mode. No “search” was done on any of the devices, other than for the specific encryption on the laptop, until the warrants were authorized, so no “fruit” was gained until the warrants were executed. See Exhibit A. The Defendant’s argument seems to allude to the notion that he cannot “be compelled...to be a witness against himself” and that the disclosure of his passwords, pursuant to the warrants, would violate his constitutional rights. U.S. CONST. Amend. V. This argument cannot survive as the Supreme Court has already weighed in and negated the Defendant’s position.

In *Fisher v. United States*, the Supreme Court established a framework for the compulsion of acts that lead to governmental knowledge of nontestimonial information. *Fisher v. United States*, 425 U.S. 391 (1976); See Orin Kerr, *Compelled Decryption and the Privilege Against Self-Incrimination*, TEX. L. REV. 97(4), 767 (2019). In *Fisher*, the Court was asked to answer whether the production of tax documents was testimonial. Ultimately, the Court held that forced production did

¹ So the Court is clear, no passwords or any type of information was provided by the Defendant, as it relates to the two Western Digital Hard drives. The United States’ position is that all information from those two devices was lawfully seized and searched.

not violate the Fifth Amendment and provided guidance on assessing whether a compelled act is testimonial in nature. To be testimonial, the act must involve “tacit averments” that have “communicative aspects.” *Fisher*, 425 U.S. at 410. To implicate the Fifth Amendment, the compelled act must force a person “to disclose the contents of his own mind” and “convey [] information to the Government.” *Doe v. United States*, 487 U.S. 201, 208-11(1988). Furthermore, the testimony must be incriminating. *See Hiibel v. Sixth Judicial Dist. Court*, 542 U.S. 177, 190 (2004).

The Supreme Court further held that testimonial acts may be compelled when their testimonial content is already known. *Fisher*, 425 U.S. at 411. When the compelled act “adds little or nothing to the sum total of the Government’s information,” any implied testimony is a “foregone conclusion” which does not violate the Fifth Amendment. *Id.*; Kerr, *Compelled Decryption and the Privilege Against Self-Incrimination* at 773. “The fact that government action leads to the acquisition of contents of the [devices] does not raise Fifth Amendment problems, *Fisher* explains, because the contents of the [devices] are not themselves compelled.” Kerr, *Compelled Decryption and the Privilege Against Self-Incrimination* at 777, n. 55 (citing *Fisher*, 425 U.S. at 409-10). “The question is not of testimony but of surrender.” *Fisher*, 425 U.S. 411 (citing *In re Harris*, 221 U.S. 274, 279 (1911)). Here, forcing the Defendant to enter a password so as to access the contents of an electronic device does not violate the Fifth Amendment as the

only implied assertion from the Defendant is that the Defendant knows the password to the device. Compelling the password “adds little or nothing to the sum total of the Government’s information” as the United States is aware that the Defendant knows the passwords to his own devices. *Fisher*, 425 U.S. at 411. The Defendant’s knowledge of his passwords is therefore a foregone conclusion and the compelled production of those passwords would then allow access to the electronic devices in question. Despite insight from the Supreme Court, the Defendant’s arguments seem to equate the act of decrypting a device with the act of collecting and handing over the files contained within it. Kerr, *Compelled Decryption and the Privilege Against Self-Incrimination* at 770. It is clearly not so.

Further, on May 17, 2021, the United States Supreme Court declined to hear a case out of New Jersey, *Andrews v. New Jersey*, U.S. Supreme Court, No. 20-937, that asked the Justices to weigh whether the 5th Amendment protects individuals from being forced to disclose their digital device passcodes to law enforcement.²

Lower courts have used similar logic to force a defendant to produce electronic passwords. The Third Circuit recently upheld a contempt citation against a suspect for refusing to produce passwords for electronic devices thought to contain

² In *State v. Andrews*, 243 N.J. 447 (N.J. August 10, 2020), the Supreme Court of New Jersey held that the Fifth Amendment did not shield the defendant from the compelled disclosure of his passcodes when the electronic devices were owned or operated by the defendant and in his possession when seized by the government.

child pornography. *Apple Mac Pro Comp.*, 949 F.3d 102. In that case, after the defendant refused to produce passwords, federal investigators obtained an All Writs Act order compelling the passwords. *Id.* at 105. The Magistrate Judge held that because the Government possessed the devices and knew of their contents, “decryption of the devices would not be testimonial for purposes of the Fifth Amendment[.]” *Id.* After his Motion to Quash was denied, the defendant further refused to unlock his electronic devices which led to the district court holding him in contempt. On appeal, the Third Circuit affirmed the district court’s ruling, stating “the Decryption Order did not implicate the Fifth Amendment privilege against self-incrimination because the information that would be conveyed...that he knows the requisite passwords – was a foregone conclusion.” *Id.* at 112.

A similar conclusion was reached by a district court when a defendant declined to decrypt electronic devices during a federal fraud investigation. *United States v. Fricosu*, 841 F. Supp. 2d 1232 (D. Colo. 2012). In *Fricosu*, the defendant’s encrypted electronic devices were seized pursuant to a search warrant and the Government sought a writ to require their decryption so as to produce their contents. The court granted the Government’s application to compel decryption under the All Writs Act, holding that the Government had proved, by a preponderance of the evidence, that the defendant owned the electronic devices or was the sole user of them. *Id.* at 1238; *See also United States v. Gavegnano*, 305 F. App’x 954, 956 (4th

Cir. 2009) (“Any self-incriminating testimony that he may have provided by revealing the password was already a ‘foregone conclusion’ because the Government independently proved that [the defendant] was the sole user and possessor of the computer.”). The court reasoned that “[w]here the existence and location of the documents are known to the government, no constitutional rights are touched, because these matters are a foregone conclusion[.]” *Id.* at 1236 (citing *In re Grand Jury Subpoena (Boucher)*, No. 2:06-mj-91, 2009 U.S. Dist. LEXIS 13006, *3 (D. Vt. 2009) (quoting *Fisher*, 425 U.S. 391)).

Contrarily, the Eleventh Circuit has held that a defendant could not be compelled to provide passwords to electronic devices in the event the Government was unaware of what was to be found on the devices. *See United States v. Doe (In re Subpoena Duces Tecum)*, 670 F.3d 1335 (11th Cir. 2012). However, even in that case where the court ruled in favor of the defendant, the court noted that the foregone conclusion doctrine applies when “the Government can show with reasonable particularity that, at the time it sought to compel the act of production, it already knew of the materials[.]” *Id.* at 1346 (internal quotations omitted). In *Doe*, the court found that the government failed to show “that encrypted files exist on the drives, that [the defendant] has access to those files, or that he is capable of decrypting the files.” *Id.* At 1349. The primary difference between *Doe* and *Fricosu* is the Government’s knowledge of what is to be found on the encrypted devices. In *Doe*,

the Government did not know what was on the computer, so to compel the defendant to tender the passwords would be to compel him to use “the contents of his own mind.” *Id.* at 1345. In *Fricosu*, the Government already knew what files were on the computer. See Jody Goodman, *Forced Data Decryption: Does It Violate the Fifth Amendment?*, CRIMINAL JUSTICE, 27(4) (2013).

In the instant case, there is little question that the devices are in fact owned by the Defendant, or alternatively, he is at least the sole user. The electronic devices were located, and ultimately removed, from the Defendant’s luggage, which was in his possession during the course of an international flight. The Defendant was detained immediately following his departure from the flight so there is little chance the Defendant was able to clandestinely hide his ownership of the devices. Furthermore, as seen in the video recordings of the interrogation, the Special Agents made known to the Defendant that they were well aware of the information contained on his electronic devices, including his emails, banking records, and WeChat. [MVI_0022.MP4 at 00:51-05:10, 20:20-22:45, 28:48-29:15]. Even if there is debate as to the specifics of what the agents knew at the time of the interrogation, “[t]here is little question here but that the [G]overnment knows of the existence and location of the computer’s files.” *Fricosu*, 841 F. Supp. at 1236. The “fact that [the Government] does not know the specific content of any specific documents is not a barrier to production.” *Id.* (citing *Boucher*, 2009 U.S. Dist. LEXIS 13006, *3).

Consequently, compelling the Defendant to produce the passwords to the electronic devices seized incident to his arrest cannot be testimonial as there is no conveyance of “some explicit or implicit statement of fact that certain materials exist” on the devices. *Doe*, 670 F.3d at 1345. The Defendant’s Fifth Amendment right against self-incrimination cannot possibly be violated through the tendering of the passwords pursuant to the search warrants because 1) the electronic devices are owned and used by the Defendant; 2) the special agents were aware of information contained within the devices; 3) it is a foregone conclusion that the Defendant knows the passwords to the devices he owns and operates, and; 4) valid search warrants were issued for the devices and no search for information was done prior to the authorization of the warrants. As such, any information derived from the searches of the devices in question is unquestionably admissible.

The case law clearly supports the United States’ position that regardless of the Defendant’s consent, the information recovered from the electronic devices is admissible as the production of the passwords could be compelled, thus giving the United States access to the information within. The decryption of the electronic devices cannot be testimonial in nature as it is a foregone conclusion the Defendant knows the passwords to his own devices and “adds little or nothing to the sum total of the Government’s information.” *Fisher*, 425 U.S. at 411. The devices are not “useless” as the Defendant alleges as valid search warrants were issued thereby

providing the agents opportunity to access the devices one way or another. (Defendant's Reply at 4). Furthermore, if the defendant had declined to provide the passwords, the agents would have requested in the warrant for the password and biometrics to be provided, which the United States believes the U.S. Magistrate Judge would have authorized.

III. Conclusion

As previously stated, the United States asserts that the Defendant intelligently and voluntarily waived his rights and freely consented to the search of his electronic devices. However, should the Court disagree, for the foregoing reasons, the United States respectfully requests that the Court still find that suppression of evidence derived from the Defendant's electronic devices would be improper. Valid search warrants were issued and, as a result of the search warrants, had the Defendant not provided the special agents with the passwords to the devices, the electronics would still have been accessible by compelling the Defendant to produce the passwords. The United States further requests the Court find that compelling the Defendant to decrypt his electronic devices in no way violates his Fifth Amendment right against self-incrimination as tendering the passwords is not testimonial since it is a foregone conclusion that the Defendant knows the passwords to his own devices.

The United States requests the Court deny the Defendant's Motion to Suppress in its entirety.

Respectfully submitted,

Jennifer Lowery
Acting United States Attorney

BY: /s/ S. Mark McIntyre
S. Mark McIntyre
Assistant United States Attorney

/s/ Carolyn Ferko
Carolyn Ferko
Assistant United States Attorney

John C. Demers
Assistant Attorney General

/s/ Matthew J. McKenzie
Matthew J. McKenzie
Trial Attorney
U.S. Department of Justice National
Security Division
Counterintelligence & Export Control
Section

CERTIFICATE OF SERVICE

I certify that the United States' Response to Defendant's Reply to the United States' Response to Defendant's Motion to Suppress was served on counsel for the defendant via e-mail on June 24, 2021.

/s/ Carolyn Ferko
Carolyn Ferko
Assistant United States Attorney

/s/ S. Mark McIntyre
S. Mark McIntyre
Assistant United States Attorney